UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/462,615	01/10/2000	YASUSHI KATSUMATA	7246/58772	5312

7590 11/15/2005

JAY H MAIOLI
COOPER & DUNHAM
1185 AVENUE OF THE AMERICAS
NEW YORK, NY 10036

EXAMINER	
TRUONG, THANHNGA B	
ART UNIT	**PAPER NUMBER**
2135	

DATE MAILED: 11/15/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/462,615	KATSUMATA ET AL.	
	Examiner	Art Unit	
	Thanhnga B. Truong	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10/11/2005 (RCE)*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-37* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-37* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *10 January 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on October 11, 2005 has been entered. Claims 1-37 are pending. Claims 1-2, 14-15, and 27 are amended by the applicant.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Burns et al (US 5,931,947), in view of Cooper (US 5,737,516), and further in view of Houvener et al (US 6,070,141).

a. *Referring to claim 1:*

i. Burns teaches:

(1) a first identification storing which first identification data that is unique an equipment and second identification data corresponding said first identification data been stored, wherein said first identification storing unit is formed in a single integrated circuit **[i.e., referring to Figure 1, the device 1 also includes a storage media 8 and a request processor 9. The storage media 8 contains a subscriber list 10 and an object repository 11. The subscriber list 10 includes the subscriber ids of the clients that are able to create objects on the device, while the object repository 11 houses the network objects. Each object will have a**

unique id that will never be used again on this device even if the object is deleted. (column 6, lines 19-26)];

(2) a first transmitting/receiving transmitting distribution request data together with said first identification data read out from said first storing unit receiving transmitted data **[i.e., referring again to Figure 1, the request processor 9 receives requests from the network, services them, and returns responses as provided in the flowchart of Figure 4. A request is a command sent by a client to a network storage device to access data stored on it (column 6, lines 27-31)];**

(3) a first data storing unit for storing the data received said first transmitting/receiving unit **[i.e., the network storage devices of Burns' invention are used as repositories of remotely encrypted data, where each network storage device is an independent entity. All encryption is done by the network clients (the components of the network that request data from the devices), so that data that travels over the network is stored encrypted (column 5, lines 48-54)];**

(4) a first signal processing unit for performing decoding process to the data read out from said first data storing unit based on said second identification data stored said first identification storing unit, wherein said first signal processing unit is formed in said single integrated circuit **[i.e., all encryption is done by the network clients (the components of the network that request data from the devices), so that data that travels over the network is stored encrypted. The advantage of this approach is that data is encrypted or decrypted by the clients as opposed to having the encryption being done at both the devices and the clients (column 5, lines 51-57). Furthermore, Figure 3 provides a block diagram depiction of a plurality of data processing system attributes which may be utilized to uniquely identify a particular data processing system (whether a stand-alone or a node in a distributed data processing system), and which further can be utilized to generate in the machine identification value which is utilized to derive or generate a temporary access product key which may be utilized to gain access to**

an encrypted product for a particular predefined trial interval. A data processing system may include a particular system bus 60 architecture, a particular memory controller 74, bus controller 76, interrupt controller keyboard mouse controller 80, DMA controller 66, VGA video controller 82, parallel controller 84, serial controller 86, diskette controller 88, and disk controller 82. Additionally, a plurality of empty or occupied slots 106 may be used to identify the particular data processing system. Each particular data processing system may have attributes which may be derived from RAM ROM 68, or CMOS RAM 72 (column 7, lines 50-67 through column 8, line 1)];

(5) a first control unit for performing an operation to allow the data received said first transmitting/receiving unit to be stored into said first data storing unit and controlling the decoding process of the data read out from said first data storing unit by said first signal processing unit **[i.e., a process controller, or a distributed computing system, which includes data storage and suitable programming means for operating in accordance with the devices and methods to be disclosed, also falls within the spirit and scope of the invention (column 5, lines 16-21). In addition, Figure 1 is a block diagram of a network storage device 1, which is part of the secure array of encrypted devices, according to the invention. The device 1 is one of many similar devices attached to a network 2, along with the network clients (not shown). Each storage device 1 has a device owner for controlling access to the device's data (column 5, lines 60-65)]**;

(6) a second transmitting/receiving for receiving said first identification data and said distribution request data transmitted from said first transmitting/receiving unit and for transmitting the data; a second data storing unit in which a plurality of data stored and which outputs data corresponding said distribution request data; an identification database (i.e., storage device) storing unit which stores an identification database indicating a relationship between a plurality of first identification data and a plurality of second identification data; a second signal processing unit for performing an enciphering process the data outputted from said second data storing unit based on second identification data read out from said

identification database corresponding to said first identification data transmitted from said first transmitting/receiving unit; and a second control performing a reading control of said second identification data from said second storing unit based on said distribution request data and said first identification data which were transmitted and performing reading control of the data from said second data storing unit based on said distribution request data, wherein the data enciphered on the basis of said second identification data transmitted through said second transmitting/ receiving unit decoded by said first signal processing unit, and said first identification storing unit and said first signal processing unit are formed in said single integrated circuit **[i.e., each object will have a unique id that will never be used again on this device even if the object is deleted. Details on the layout of the network objects are described below in reference to in Figure 2 (column 6, lines 24-26). As each of the distributed file system would be a mirror image of each other, then it would contain a second data storing unit for storing a plurality of data (see Abstract, that is a plurality of data objects) from the first transmitting/receiving unit. It would also contain an encryption unit for encrypting data to be sent over an insecure network wherein the data enciphered is based on second identifier (column 6, lines 38-39). In addition, FIG. 4 is a block diagram depiction of a routine for encrypting software objects. The binary characters which make up software object 201 are supplied as an input to encryption engine 205. Real key 203 is utilized as an encryption key in encryption engine 205. The output of encryption engine 205 is an encrypted software object 207. Encryption engine 205 may be any conventional encryption operation such as the published and well known DES algorithm; alternatively, the encryption engine 205 may be an exclusive-OR operation which randomizes software object 201 (column 8, lines 57-67)].**

ii. Although Burns teaches the claimed subject matter, as well as the network client performs all encryption and decryption of data and metadata (column 3, lines 52-53) and storage device 1 as shown in Figure 1, he does not explicitly mention:

(1) the decryption process is performed within the same circuit, unit, engine, or device.

(2) a relationship between a plurality of first identification data and a plurality of second identification data

iii. On the other hand, Cooper teaches:

(1) Figure 20 depicts in block diagram form the technique of utilizing a plurality of inputs within the user-controlled data processing system to derive the real key, which may be utilized to decrypt an encrypted software object.

iv. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) have modified the invention of Burns with the teachings of Cooper, if indeed it wasn't inherent in Burn's data decryption device, for securing access to software objects, and in particular to techniques for temporarily encrypting and restricting access to software objects **(column 1, lines 37-39 of Cooper).**

v. The ordinary skilled person would have been motivated to:

(1) have modified the invention of Burns with the teachings of Cooper since it is also possible that unscrupulous individuals may post keys to publicly-accessible bulletin boards to allow great numbers of individuals to become unauthorized users. Typically, these types of breaches in security cannot be easily prevented, so vendors have been hesitant to distribute software for preview by potential customers **(column 2, lines 20-25 of Cooper).**

vi. And Houvener teaches:

(1) The invention provides a system and method of assessing the quality of an identification transaction. The method comprises registering a plurality of persons to be identified by providing at least two identification units corresponding to each person and storing the identification units in an identification database **(column 3, lines 14-19 of Houvener).**

vii. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) have modified the invention of Burns with the teachings of Houvener, if indeed it wasn't inherent in Burn's storage device as shown in Figure 1, for identity verification purposes **(column 1, line 14-15 of Houvener).**

viii. The ordinary skilled person would have been motivated to:

(1) have modified the invention of Burns with the teachings of Houvener to protect any situation where the possibility for identity-based fraud exists, such as banking transactions, welfare distributions, voting, firearms sales, health care, airline tickets, immigration and naturalization, and other law enforcement situations **(column 1, lines 24-29 of Houvener).**

b. *Referring to claim 2:*

i. Burns further teaches:

(1) wherein accounting information is transmitted from said first transmitting/receiving unit to said second transmitting/receiving unit, said second control controls the reading operation of said second identification data from said identification database (i.e., storage device) storing unit based on said transmitting accounting information **[i.e., typically, the network storage device is shipped with a device owner key in firmware and the owner is given the key with the device upon purchase. All keys pertaining to access to the device are derived from the owner key (column 8, lines 6-9)].**

c. *Referring to claim 3:*

i. Burns further teaches:

(1) for performing an enciphering process to the data which is written into said second data storing unit based on enciphering data, and wherein the data enciphered by said means for performing an enciphering process is written into said second data storing unit, and when the data data storing unit based on said distribution request data and read out from said second transmitted from said second transmitting/receiving said first transmitting/receiving unit, said enciphering data is enciphered by said second identification data and said second signal processing and transmitted together with the data read out from said second data storing unit **[i.e., all encryption is done by the network clients (the components of the network that**

request data from the devices), so that data that travels over the network is stored encrypted. The advantage of this approach is that data is encrypted or decrypted by the clients as opposed to having the encryption being done at both the devices and the clients. In order for the system to revoke access to an object (file or directory) on the device, the object must be re-encrypted (column 5, lines 50-59 and Table 2)].

d. *Referring to claim 4:*

i. Burns further teaches:

(1) wherein said first signal processing unit decodes the data transmitted from said second transmitting/receiving unit and said enciphering data by said second identification data stored in said first storing unit and performs decoding process of an encryption performed by said enciphering data to the data decoded based on the decoded enciphering data **[i.e., each file data object, also shown in Figure 2, preferably includes the common network object header followed by encrypted file data. The network client is responsible for performing encryption and decryption of file data. Encrypted file data is seen simply as a random string of bytes by the network storage device (column 7, line 36-37)].**

e. *Referring to claim 5:*

i. Burns teaches the claimed subject matter, but Burns does not clearly mention:

(1) wherein said first control unit performs an accounting process based on said enciphering data .

ii. However, Cooper teaches:

(1) the use of the controller both to identify data being processed, i.e., requests to a network storage device need to be authenticated and guaranteed for freshness. The storage device also enforces access rights listed in Table 1 above. A request that will change the state of the storage will be authenticated by the device, rather than the client. The results of a request needs to be authenticated by the network client to prevent spoofing problems. Furthermore, all requests and responses must also be guaranteed fresh to prevent replays (i.e., presenting of copies of requests

and responses by some other entities in the system to impersonate the true requester or recipient) **(column 7, lines 57-67).**

iii. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) have put accounting process via the controller as taught by Cooper under the general database exchange and purchasing functions of Burns' invention because the controller keeps track of the data identification and owner.

iv. The ordinary skilled person would have been motivated to:

(1) have put accounting process via the controller as taught by Cooper under the general database exchange and purchasing functions of Burns' invention to insure the owner is paid for his data placing the accounting under the control of the controller which keeps track of data ID would prevent duplication of resources and increase the throughput in the event large amount of data are exchanged.

f. *Referring to claim 6:*

i. Burns further teaches:

(1) wherein said enciphering data has a data portion which dynamically changes and said control discriminates said dynamically changing data portion, at every predetermined time, in said enciphering data stored in said first data storing unit and transmitted together with the data from said second transmitting/receiving unit **[i.e., there are two types of network objects: directory data objects and file data objects. File data objects contain all or part of the file data of a file. Directory data objects contain all or part of the directory entries of a directory. Each network object on a device is identified by a unique object id. In addition, both types of objects are transmitted over the network (column 5, lines 30-45) and as these data objects must be handled differently, the controller must be able to respond dynamically depending on which type of data object is being sent. Thus Burns discloses a control unit (i.e., a controller) which dynamically responds to changing data portion].**

g. *Referring to claim 7:*

i. This claim has limitations that is similar to those of claims 1 and 6, thus it is rejected with the same rationale applied against claims 1 and 6 above.

h. *Referring to claim 8:*

i. Burns further teaches:

(1) wherein said first control unit inhibits the reading operation of the data from said first data storing unit when the discrimination result of said dynamically changing data portion indicates that said enciphering data is not correct **[.e., H(request) is the hash of the request that generated the error. ecode is the error code that represents why the request failed. edata is error data that gives specific details about why the request failed. keydata is the data that corresponds to the key used it the request. K is the key that was used in the request. Note, if the request failed due to an invalid key used in the request, keydata and K are not used (column 9, lines 63-67)].**

i. *Referring to claim 9:*

i. This claim has limitations that is similar to those of claim 5 and column 8, lines 1-9, thus it is rejected with the same rationale applied against claim 5 and column 8, lines 1-9 above.

j. *Referring to claim 10:*

i. This claim has limitations that is similar to those of claims 5 and 9, thus it is rejected with the same rationale applied against claims 5 and 9 above.

k. *Referring to claim 11:*

i. This claim has limitations that is similar to those of claim 5 and column 8, lines 1-9, thus it is rejected with the same rationale applied against claim 5 and column 8, lines 1-9 above.

ii. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) modify Burns to include elapse time as a measured parameter because with the concern for data freshness the time which the data update is made becomes important, especially if the site is being billed for the update, that is the site does not wish to pay for an out of date update.

iv. The ordinary skilled person would have been motivated to:

(1) modify Burns to include elapse time as a measured parameter because the controller is the place which takes care of the billing and so this would be the most efficient place to control data reading for updates.

l. *Referring to claims 12-13:*

i. Burns further teaches:

(1) The limitation of encryption device for decoding data based on the destination is being move and wherein the control unit deletes data when movement in data storage unit is finished **[i.e., network objects are used to store data on the storage devices. There are two types of network objects: directory data objects and file data objects. File data objects contain all or part of the file data of a file. Directory data objects contain all or part of the directory entries of a directory. Each network object on a device is identified by a unique object id. Note that an object id is not reused even if the corresponding object is deleted. Each object has an object administrator key, which is used to create the lookup, read, extend, delete, and update keys for the object. The backup key is derived from the owner key 3 and is used to enumerate the objects on the storage device 1 and read those objects (column 6, lines 46-58)].**

m. *Referring to claims 14-26 and 35-37:*

i. These claims have limitations that are similar to those of claims 1-13 and 11, thus they are rejected with the same rationale applied against claims 1-13 and 11 above.

o. *Referring to claims 27 and 29-34:*

i. These claims have limitations that are similar to those of claims 1-2 and 6-10, thus they are rejected with the same rationale applied against claims 1-2 and 6-10 above.

Conclusion

4. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thanhnga (Tanya) Truong whose telephone number is 571-272-3858.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached at 571-272-3859. The fax and phone numbers for the organization where this application or proceeding is assigned is 571-272-8300.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

TBT
November 7, 2005

Primary Examiner
Art Unit 2135